

REPORT DOCUMENTATION PAGE

*Form Approved
OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

| | | | | | |
|--|-----------------------------|--------------------------------|--------------------------------------|--|--|
| 1. REPORT DATE (DD-MM-YYYY) 14-02-2005 | | 2. REPORT TYPE FINAL | | 3. DATES COVERED (From - To) | |
| 4. TITLE AND SUBTITLE INFORMATION OPERATIONS: WHERE NEXT? | | | | 5a. CONTRACT NUMBER | |
| | | | | 5b. GRANT NUMBER | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) LCDR David R. Buchholz, USN Paper Advisor (if Any): LtCol Derrill T. Goldizen, USAF | | | | 5d. PROJECT NUMBER | |
| | | | | 5e. TASK NUMBER | |
| | | | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | |
| 12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A: Approved for public release; Distribution is unlimited. | | | | | |
| 13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | | | | | |
| 14. ABSTRACT This paper addresses the "ownership" of joint information operations (IO) by asking if U.S. Strategic Command is the right combatant commander to coordinate all Department of Defense information operations. Doctrine already addresses the issue of combatant commander responsibility for ensuring IO is planned and executed in the respective commands but an IO vacuum exists with respect to standardized IO training and integration across the combatant commands. For this reason and others there is a compelling argument for the major responsibility for DOD information operations integration to fall under the control of U.S. Joint Forces Command. First is provided, an explanation on how U.S. Strategic Command became the IO integrator for DOD IO. This is followed by the definition of joint IO as found in Joint Publication 3-13. Then, several examples highlight the importance of IO integration to regional commanders. Finally, the command missions of U.S. Strategic Command and U.S. Joint Forces Command are analyzed to illustrate why U.S. Joint Forces Command is most suited to play the major role in the integration and projection of joint IO. | | | | | |
| 15. SUBJECT TERMS Information operations, IO, joint information operations | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES 19 | 19a. NAME OF RESPONSIBLE PERSON Chairman, JMO Dept | |
| a. REPORT UNCLASSIFIED | b. ABSTRACT UNCLASSIFIED | | | c. THIS PAGE UNCLASSIFIED | 19b. TELEPHONE NUMBER (include area code) 401-841-3556 |

**NAVAL WAR COLLEGE
Newport, R.I.**

INFORMATION OPERATIONS: WHERE NEXT?

by

David R. Buchholz

Lieutenant Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements for the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

14 February 2005

**LtCol Derrill T. Goldizen, USAF
Faculty Advisor**

Abstract

This paper addresses the “ownership” of joint information operations (IO) by asking if U.S. Strategic Command is the right combatant commander to coordinate all Department of Defense information operations. Doctrine already addresses the issue of combatant commander responsibility for ensuring IO is planned and executed in the respective commands but an IO vacuum exists with respect to standardized IO training and integration across the combatant commands. For this reason and others there is a compelling argument for the major responsibility for DOD information operations integration to fall under the control of U.S. Joint Forces Command.

First is provided, an explanation on how U.S. Strategic Command became the IO integrator for DOD IO. This is followed by the definition of joint IO as found in Joint Publication 3-13. Then, several examples highlight the importance of IO integration to regional commanders. Finally, the command missions of U.S. Strategic Command and U.S. Joint Forces Command are analyzed to illustrate why U.S. Joint Forces Command is most suited to play the major role in the integration and projection of joint IO.

*The clever combatant imposes his will on the enemy, but does not allow the enemy's will to
be imposed on him.¹*

Sun Tzu

Introduction

The practice (if not the concept) of Information Operations (IO)¹ is deep-rooted in history, from at least 1200 B.C. when the Greeks constructed the Trojan Horse to gain entrance to Troy,² to modern operations in Kosovo and Iraq. Information operations and information warfare, initially classified concepts, have only officially been embedded in U.S. joint doctrine since 1998 with the first publication of Joint Publication 3-13, *Joint Doctrine for Information Operations* (9 October 1998). Since then, doctrine has remained relatively unchanged but “ownership” of joint IO has changed four times. Although the responsibility for coordination of Department of Defense IO currently resides with U.S. Strategic Command (USSTRATCOM),³ since 1997, joint information operations has been delegated to a succession of unified commanders through their command of the Joint Command and Control Warfare Center (JC2WC), later to become the Joint Information Operations Center (JIOC).

Should coordination of joint information operations as a stated mission require direct oversight of a single unified combatant commander? Does USSTRATCOM provide the best fit? Just as there are advantages with USSTRATCOM as the joint IO integrator there are valid arguments for the responsibility of joint IO integration to fall elsewhere.

Joint Publication 3-13 states that IO should be an integral part of all joint military operations and specifically identifies organizing, planning and coordinating information

¹ Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, DC: 9 October 1998), VII, defines information operations as actions taken to affect adversary information and information systems while defending one’s own information and information systems.

operations as the responsibility of the Joint Force Commander.⁴ If IO is already doctrinally mandated to be an integral part of all joint military operations, then why should Department of Defense IO, as a mission, be assigned to a specific unified commander? Responsibilities for DOD IO integration should be placed under the combatant commanders with the best tools to accomplish the mission. Doctrine already addresses the issue of combatant commander responsibility for ensuring IO is planned and executed in the respective commands but an IO vacuum exists with respect to standardized IO training and integration across the combatant commands. For this reason and others there is a compelling argument for the major responsibility for Department of Defense information operations integration to fall under the control of U. S. Joint Forces Command (USJFCOM).

First is provided, an explanation of how USSTRATCOM became the IO integrator for Department of Defense IO. This will be followed by the definition of joint IO as found in Joint Publication 3-13. Then, several examples will highlight the importance of IO integration to regional unified commanders. Finally, the command missions of USSTRATCOM and USJFCOM will be analyzed to illustrate why USJFCOM is the command most suited to play the major role in the integration and projection of joint IO.

Evolution of Joint IO

How did joint IO evolve to where it is today? The formal “trail of IO” begins, in 1993, when the mission for joint information operations integration was assigned to the Joint Command and Control Warfare Center (JC2WC) at the time when the JC2WC reported directly to the Joint Chiefs of Staff (JCS).⁵ The Defense Initiative of 1997 removed several agencies from the direct auspices of the JCS and, in 1998, resulted in the JC2WC, and subsequently IO, falling under U.S. Atlantic Command.⁶ In October 1999, when U.S

Atlantic Command became U.S. Joint Forces Command, the Joint Command and Control Warfare Center became the Joint Information Operations Center (JIOC) and was realigned under U.S. Space Command (USSPACECOM).⁷ When the 2002 Unified Command Plan merged USSPACECOM with USSTRATCOM, the JIOC and its core mission of joint information operations support to the unified commanders was transferred to USSTRATCOM as well. At this point, it was advocated that USSTRATCOM be designated the IO integrator for regional IO, to provide a global perspective and coordinate with other government agencies. Subsequently, USSTRATCOM's mission was modified, specifically delineating its role to coordinate all DOD space and strategic information operations capabilities to meet both deterrent and decisive national security objectives.⁸ Former USSTRATCOM commander, Admiral James O. Ellis Jr. stated, "Now, for the first time, information operations are going to be assigned to somebody. They've never been [under] a unified commander before."⁹

Having traced the brief history of joint IO and its eventual inclusion into Strategic Command's mission, has responsibility for joint information operations finally reached the appropriate resting spot?

What is Information Operations?

There exists a perception that IO is strictly technology driven. *Information Operations: The Hard Reality of Soft Power* published by the Joint Forces Staff College, does a thorough job of explaining what IO is and what it is not. One of its observations is that, "To many people, IO is simply computer warfare...IO is really about much more than that."¹⁰ Information operations, as defined by Joint Publication 3-13, involve actions taken to affect adversary information and information systems while defending one's own information and

information systems. They apply across all phases of an operation to the full range of military operations, and at every level of war--strategic, operational, and tactical.¹¹

“It [information operations] is perhaps best defined by describing its objective: to cause a desired change in behavior of an adversary by targeting his mind rather than his body.”¹²

Information operations can be offensive or defensive and are mutually supportive.

Offensive information operations integrate several assigned and supporting capabilities and activities to affect adversary decision makers and achieve or promote specific objectives.¹³ Capabilities and activities of IO include, but are not limited to, deception, electronic warfare, operations security, psychological operations, computer network attack, public affairs, and civil affairs. The integration of these capabilities and activities to affect adversary decision makers constitutes IO. To attempt to utilize all of these capabilities leads to a common complaint that “because its definition is so broad, at once IO is everything and it is nothing. While one can try to use all eight capabilities and related activities to conduct an operation, more often than not, a good IO plan will probably only incorporate a few of these warfare areas.”¹⁴

Defensive information operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO is conducted through information assurance, operations security, physical security, counterdeception, counterpropaganda, counterintelligence, electronic warfare and special information operations.¹⁵

How can IO Change the Battlespace?

Why are unified commanders tasked with integrating information operations across all phases of an operation and at every level of warfare? Why should they be concerned about

the correct application of IO in their geographic areas of responsibility? The following four historical examples, covering conflicts in four different geographic regions spanning 60 years, will highlight how IO, if successfully implemented can be a force multiplier and mission enabler. They will also shed light on the difficulties and consequences encountered if an IO strategy is not properly implemented.

IO in World War II

In October 1944, during World War II, the Japanese used “IO”, with heavy emphasis on deception, as a force multiplier during the Battle of Leyte Gulf. The outnumbered Japanese Imperial Navy, attempting to repel the allied invasion of the Philippines, specifically targeted the decision making of the Third Fleet Commander, Admiral William “Bull” Halsey. The Japanese attempted to exploit the eagerness of Admiral Halsey to pursue and destroy the Japanese aircraft carriers. Relying on this intelligence, the Japanese Imperial Navy created a Northern (diversionary) Force that included its aircraft carriers and successfully lured Halsey away from the San Bernadino Strait. This enabled the Japanese Center Force to sail through the San Bernadino Strait virtually unopposed and seriously threaten the allied amphibious landing on Leyte.

“Nobody at Pacific Fleet Headquarters in Hawaii was surprised at Halsey’s northward dash. Given a choice of objectives, he could always be expected to go after carriers, the warships with the longest reach and hardest punch.”¹⁶ Although this propensity of Halsey was not viewed as a vulnerability by friendly forces, it was certainly exploited by the Japanese. Only the defensive efforts of a severely outnumbered and outgunned allied naval task force and the inexplicable retreat of the central Japanese force prevented a catastrophic attack on the unguarded flanks of the allied amphibious landing. There were command and

control deficiencies that contributed to the unguarded San Bernadino straight but regardless, the Japanese, through a successful information operations strategy, were able to manipulate the decision of a senior U.S. decision maker, enabling them to shape the battlefield and provide an opportunity for success where none had existed previously.

IO in Iraq

Information operations (at the time called Command and Control Warfare (C2W)) were used successfully in 1991 during Operation DESERT STORM. Applying information operations, the Allied coalition in DESERT STORM “systematically demoralized Iraq’s frontline troops, crippled Iraq’s integrated air defenses, blinded its ability to target coalition forces, shut down its propaganda machine, and totally disrupted military communications from the national to the operational level.”¹⁷ The synchronized integration of psychological operations, physical destruction, deception and electronic attack directly lead to the liberation of Kuwait and the swift defeat and surrender of Iraq’s military forces.

Balkans: IO Success or Failure?

In 1998, information operations were utilized extensively during Operation NOBLE ANVIL, successfully and unsuccessfully. Operation NOBLE ANVIL was the U.S. contribution to NATO’s larger Operation ALLIED FORCE which attempted to expel the Serbian forces from Kosovo. A draft briefing attributed to Admiral James Ellis, the Commander of ALLIED FORCE and Joint Task Force NOBLE ANVIL, described IO as “at once a great success...and perhaps the greatest failure of the war.” Admiral Ellis continued:

“The enemy was much better at this [public affairs] than we were...and far more nimble. The enemy deliberately and criminally killed innocents by the thousands, but no one saw it...we accidentally killed innocents, sometimes by the dozens, and the world watched on the evening news. We were continuously reacting, investigating, and trying to answer ‘how could this happen?’”¹⁸

IO successes included the formation of the first IO cell at the JTF level and effective employment of psychological operations. However, a general lack of IO understanding by warfighters and a resounding defeat in the public affairs battle led to missed opportunities. NATO was susceptible to deception and denial, lacked adequate operations security and conducted predictable air attacks. Additionally, the Serbians used the internet for public-affairs and propaganda purposes and to conduct information attacks against NATO countries.¹⁹

IO in Haiti

On a smaller scale, Operation UPHOLD DEMOCRACY in Haiti in 1994 highlighted several of the difficulties of conducting IO in a peacetime environment. A concerted psychological effort with a message urging the Haitian civilian and military leadership to peacefully relinquish power was initiated when U.S. forces attempted to return democratically-elected Haitian president Jean-Bertrand Aristide to power. “The Joint Task Force Haiti Assistance Group, embarked aboard the USS Harlan County, was unprepared when they entered Port-au-Prince Harbor and found a Cuban tanker blocking its assigned berth; an angry, drunken mob at the piers; and aggressive Haitian navy gunboats.”²⁰ A negative Haitian backlash resulted when it was reported that U.S. forces had been “thrown out of Haiti.” This loss in the perception management effort was a result of the failure of the military to respond to unfavorable events before the Haitians could use them for their own propaganda. Operations Security (OPSEC) was also an issue as, “despite a concerted effort to maintain OPSEC, throughout planning and executing the deployment of U.S. forces, it proved impossible to hide the fact that the 10th Mountain Division had embarked on the aircraft carrier USS Eisenhower.”²¹

As illustrated in the previous examples, IO is conducted at all levels of conflict. If carefully conceived, coordinated, and executed, IO can make an important contribution to defusing crises, reducing periods of confrontation, and enhancing the impact of informational, diplomatic, economic, and military efforts.²² These examples, covering four different geographic regions and spanning over 60 years, demonstrate how IO can positively or negatively affect the face of the “battlefield.” In Kosovo and Haiti it can be argued that the most glaring shortcoming was, not lack of planning and lack of IO tools, but rather the lack of trained and experienced personnel to implement a cohesive IO strategy that would integrate the various capabilities of IO. Proficiency can be obtained through training and experimentation. Which combatant commander can best fill the void: U.S. Strategic Command or U.S. Joint Forces Command?

U.S. Strategic Command’s Suitability as DoD’s “Joint IO Integrator”

U.S. Strategic Command controls military space operations, computer network operations, Department of Defense information operations, strategic warning and intelligence assessments as well as global strategic planning. Its stated mission is:

“to establish and provide full-spectrum global strike, coordinated space and information operations capabilities to meet both deterrent and decisive national security objectives. Provide operational space support, integrated missile defense and specialized planning expertise as well as global command and control, communications, computers, intelligence, surveillance and reconnaissance to the joint warfighter.”²³

USSTRATCOM controls two geographically separated units that are major players in the integration of information operations: the Joint Information Operations Center (JIOC) and Joint Task Force – Global Network Operations (JTF-GNO). The JIOC, operating primarily at the operational level, plays the major role in “joint IO” integration. It is responsible for the integration of IO into military plans and operations across the spectrum of conflict. Specially

tailored IO planning teams are prepared to deploy worldwide with little notice to provide IO assistance and technical support to joint commanders, joint task forces and the joint staff.²⁴

JTF –GNO coordinates and directs the defense of U.S. military computer systems and networks.² Within each theater of operation, JTF-GNO operates emergency response teams, network operation and security centers and satellite communication support centers which monitor the status of DOD information networks and defend them from any unauthorized events such as probes, scans, virus incident, or intrusion.²⁵ With its expertise and responsibility for global network operations and information assurance, JTF-GNO plays a valuable role in supporting IO strategies.

Ownership of the JIOC and the relationship between IO and computer network operations is the major link between USSTRATCOM and information operations. From the organizational history of the JIOC and the evolution of joint IO, one might assume that the JIOC was placed under USSPACECOM, and later USSTRATCOM, based on IO's association with computer network operations. If this assumption is true, then perhaps the importance of integrating the "other" capabilities of IO has been inadvertently diminished by this association. While Operation NOBLE ANVIL highlighted the importance of computer network operations, it also reinforced the requirement for a comprehensive IO strategy.

USSTRATCOM controls two capabilities upon which the vertical integration of strategic IO with operational and tactical IO are essential; global Command and Control (C2) and Intelligence, Surveillance, and Reconnaissance (ISR). While USSTRATCOM's Global Operations Center (GOC) enables the command to collaborate with other commanders and

² Joint Task Force-Global Network Operations was originally created as the JTF- Computer Network Defense in 1998 under U.S. Space Command. In 2002 it was redesignated the JTF – Computer Network Operations. With the merger of USSPACECOM and USSTRATCOM in 2002, JTF – CNO became a component of USSTRATCOM. In 2004, JTF-CNO was redesignated JTF-GNO with authorities and responsibilities for Global Network Operations and Defense.

national agencies to plan and execute worldwide missions, its ISR capability continually provides critical support to the joint warfighter.²⁶ These two capabilities in conjunction with 50 years of strategic planning expertise enable USSTRATCOM to effectively coordinate strategic IO.

U.S. Joint Forces Command’s Advantage as “Joint IO Integrator”

Two of the lessons learned from Kosovo were a general lack of IO understanding by warfighters that led to missed IO opportunities and a loss in the public affairs battle. U.S. Joint Forces Command is in an ideal position to address these issues in the effort to further the effective joint integration of IO.

U.S. Joint Forces Command, in the 2002 Unified Command Plan, was given the focus of developing transformational concepts to build the military of the 21st century. Joint Forces Command’s mission includes: Joint Force Provider, Joint Force Integrator, Joint Force Trainer, and Joint Concept Development and Experimentation.²⁷ This mission provides USJFCOM the appropriate perspective, reach, and resources to fully integrate joint IO. For example, as Joint Force Provider, USJFCOM ensures elements of the Army, Navy, Air Force and Marine Corps can operate together as specialized, task-organized teams²⁸ – an essential capability when planning and executing the employment of disparate IO capabilities each of the services brings to the fight.

As the Joint Force Integrator, USJFCOM determines how weapons and support systems, both existing and in the acquisition stage, will integrate into the plans and needs of joint commanders²⁹ – an important capability that improves the effective integration of kinetic and non-kinetic targeting options into IO strategies.

As the joint force trainer and lead for joint concept development and experimentation, USJFCOM facilitates joint military exercises, conducts assistance visits to deployed joint warfighters and captures lessons learned.³⁰ Supporting exercises and training warfighters is arguably one of USJFCOM's most important contributions to IO. The ability to collate lessons learned to improve tactics, techniques and procedures ensures the increased effectiveness of forces.

Joint doctrine assigns responsibility to joint force commanders for ensuring that key personnel responsible for planning and conducting IO receive the appropriate training. USJFCOM has been pivotal in this regard by providing combatant commanders the tools they need to train, through the development and implementation of a Standing Joint Force Headquarters Core Element (SJFHQ), the Joint National Training Capability (JNTC) and the Joint Warfighting Center (JWFC).

The SJFHQ is a 58 member team of operational planners and information warfare command and control specialists that forms the core of a joint task force headquarters command structure.³¹ Of the 58 member team, six positions are directly assigned to information operations.³²

"[The SJFHQ] provides a ready full-time team that aids in the ability to stand up a joint task force headquarters quickly," says Rear Admiral Richard J. O'Hanlon, who oversees the SJFHQ development and implementation efforts. "By providing a joint cadre of trained planners and operators who have a thorough understanding of effects based operations (EBO) and the regional commanders intent, we have found that a joint task force headquarters can come up to fighting speed quicker than we have seen in the past."³³

Joint Forces Command not only stood up the prototype SJFHQ but is also responsible for helping bring on line SJFHQ's for all geographic combatant commanders by the end of fiscal year 2005. The prototype SJFHQ will not be disbanded when all of the geographic

combatant commanders have SJFHQ's on line; the Joint Forces Command SJFHQ will continue to train new additions that rotate through the geographic combatant commands and provide assistance as necessary. Additionally, Strategic Planning Guidance for 2006 directs the establishment of another Joint Forces Command SJFHQ that will function as an operational unit.³⁴

Millennium Challenge 2002, a joint exercise hosted by Joint Forces Command, involved testing the SJFHQ and integrating information operations in rapid-decisive and effects-based operations to gain and maintain information superiority.³⁵ Early in the exercise the JTF commander recognized information operations as a capstone element of combat power, both in the lethal and nonlethal sense.³⁶ The exercise highlighted two important points consistent with a JTF and IO:

First, combatant commanders must have a strategy in place, clarify the JTF in achieving the strategy, and accept the strategy as critical to objectives. Second, the role of information operations cannot be simply an afterthought addressed immediately before a conflict. Shaping and influencing activities must occur continuously throughout peace, crisis, and combat. It is almost impossible to change a popular negative view of JTF efforts once shots are fired.³⁷

“Effective employment of IO in joint operations depends on the ability to organize and train in the manner the U.S. intends to employ military force.”³⁸ Millennium Challenge 2002 successfully validated this statement from Joint IO doctrine. If nothing else, it brought to the forefront the importance of properly training the SJFHQ; an important part of which is the integration of joint information operations throughout all levels of planning.

The Joint National Training Capability (JNTC), which is being fielded by USJFCOM, will allow for increased IO training and integration in all levels of conflict. Designed to improve the ability of U.S. forces to fight effectively as a joint and combined team, the JNTC covers the full spectrum of warfighter decision-making – from the strategic and operational

to tactical levels of war.³⁹ Admiral Giambastiani, Commander Joint Forces Command comments:

History has taught us that joint warfighting is the way of the future. The development of a JNTC will support the broader strategic goal of Department of Defense training transformation with the ultimate goal ‘to train like we fight’...the JNTC will continue to move from interoperability training at the tactical to the operational level, allowing network-centric and mission rehearsal capabilities that increase the combat power of sensors, weapons and decision making systems.⁴⁰

USJFCOM’s Joint Warfighting Center (JWFC) leads joint warfighter capability improvement through joint training. The JWFC is specifically mandated by joint doctrine “to ensure combatant command and service IO requirements are satisfied by current modeling and simulation systems and to coordinate with and assist the Joint Staff, Services, and combatant commanders in developing joint IO doctrine.”⁴¹ The JWFC Commander serves as the joint force trainer to ensure the fidelity and coordination of the military’s overall joint training efforts. The joint force trainer team and its partners revise the content and execution of training, develop advanced technologies and reshape the overall training environment to better prepare combatant command staffs, joint task forces and the individual services.⁴²

JWAC – A Step in the Right Direction

The Joint Warfare Analysis Center (JWAC), a subordinate unified command of USJFCOM provides:

operational planners with full-spectrum analytical products that are synergistic, effects-based, precision targeting options for select infrastructure networks to support planning and execution of military operations...participates in the development of net methodologies and technologies in support of joint experimentation, wargaming, precision management and other activities and coordinates directly with the staffs of all unified commands, DOD elements, combatant commands, military services, and other government departments and agencies to respond to world crises.⁴³

While the JWAC plays a major role in developing targeting options for select IO objectives, classification precludes a more in depth look to the full extent of its support.

The JWAC and the JIOC are linked by a common past. Like the JIOC, the JWAC was assigned to the Joint Chiefs of Staff until 1998, when as a result of the 1997 Defense Reform Initiative, it became a subordinate command of U.S. Atlantic Command (USACOM). In 1999 when USACOM became USJFCOM, instead of moving to USSPACECOM like the JIOC, the JWAC became an operations organization and a subordinate joint command under USJFCOM, which is where it remains today.

Information operations have been shown to be an integrating strategy which, if not in terminology at least in practice, can be documented throughout history. In order for IO to be properly implemented, realistic training is required. As shown, Joint Forces Command possesses the ability and reach to realistically prepare the warfighter to conduct information operations as doctrinally defined and thus should be the major proponent for Department of Defense information operations.

Counterarguments

It can be argued that the pieces are soon to be in place for USSTRATCOM to adequately oversee IO across the Department of Defense. USSTRATCOM's on-going reorganization will include a new functional component command for IO that will expand its expertise beyond computer network operations.⁴⁴ Questions to consider are: Do we need another joint IO command? And if so, how will the IO component command complement the JIOC? Is this a redundant level of joint IO bureaucracy? Why even raise these questions when all that is currently required is a slight reorganization of current command structures...such as assigning the JIOC to USJFCOM?

Information operations, as stated earlier, should be coordinated at strategic levels as well as at the operational and tactical levels. Since operational and tactical IO often have strategic implications, why not have USSTRATCOM carry the ball for DOD IO? Because, without major reorganization, USSTRATCOM does not possess the ability or infrastructure to be the major proponent for DOD information operations below the strategic level. The global responsibility for command and control and ISR, while retained solely by USSTRATCOM, should give USSTRATCOM the responsibility for strategic IO. But, as outlined earlier, USJFCOM controls the resources and reach to project IO to the operational commander and thus should have the largest role in projecting joint information operations. Designating USSTRATCOM as the major proponent for operational DOD IO will overextend its capability.

Recommendations

Although not formally established, the shift in responsibility for integration of Department of Defense information operations already lies heavily with USJFCOM. The largest organizational change required to complete the transformation is to move the Joint Information Operations Center from under the command of USSTRATCOM to USJFCOM. Information operations, as an integrating strategy, has too many moving parts to place them all under one roof but the JIOC, as the “heavy hitter” for integrating these “moving parts” in the joint world, should be organizationally placed where it can achieve the largest positive effect.

The JIOC, while maintaining its current strong relationships with respective combatant commanders, would be in an ideal position to assimilate IO into all unified command Standing Joint Force Headquarters (training and operational) and assist the integration of IO

into Joint Warfighting Center sponsored exercises. Additionally, the JIOC in conjunction with the JWAC would assist with bridging the gap between training and operational support.

JTF-GNO should remain with USSTRATCOM. The tentacles of JTF-GNO, including computer network attack, computer network defense and information assurance, while supporting IO strategies at all levels, reach far beyond operational and tactical IO and thus are appropriately placed with USSTRATCOM.

Conclusions

Information Operations, as currently defined, are much too complex and unwieldy for one unified combatant commander to effectively implement throughout the Department of Defense. Combatant commanders are doctrinally charged to plan, exercise and conduct IO in support of national goals and objectives; thus USSTRATCOM already plays a large part in IO.

Joint Forces Command's mission should be expanded to reflect a renewed responsibility for joint IO integration. There should not be ownership of joint IO - just the responsibility for effectively employing it. USJFCOM has the mission and the resources to collate IO lessons learned and provide standardized training and evaluation to all combatant commanders. Additionally, the JIOC's IO expertise combined with the effects-based targeting of the JWAC would provide a synergistic effect to bridge the gap between training warfighters and operationally employing information operations.

NOTES

¹“Sun Tzu on The Art of War Chapter VI.” Yuni Library, trans. Lionel Giles M.A, <<http://www.yuni.com/library/suntzu.htm>> [7 February 05].

² “National Defense University.” Lkd. Information Operations Timeline at JC2IOS page. <http://www.jfsc.ndu.edu/schools_programs/jciws/iw/io_timeline.asp> [9 January 2005].

³ “U.S. Strategic Command SNAP SHOT” Mission and Capabilities at Snap Shot page. <<http://www.stratcom.mil/factsheetshtml/SnapShot.doc>> [9 January 2005].

⁴ Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington, DC: 9 October 1998), IV-1.

⁵ Joint Command Control & Information Warfare Staff, Extracts from Information Operations: The Hard Reality of Soft Power, Naval War College, Joint Military Operations Department, NWC 3055, Chapter 1, p 15.

⁶ William S. Cohen, Defense Reform Initiative: The Business Strategy for Defense in the 21st Century, Washington, DC: Office of the Secretary of Defense, November 1997, 72-73.

⁷ Extracts from Information Operations: The Hard Reality of Soft Power, Chapter 1, p 23.

⁸ “U.S. Strategic Command SNAP SHOT” Mission and Capabilities at Snap Shot page. <<http://www.stratcom.mil/factsheetshtml/SnapShot.doc>> [9 January 2005].

⁹ William B. Scott, “‘New’ Strategic Command Could Assume Broader Roles,” Aviation Week & Space Technology 157 (October 2002): 63.

¹⁰ Extracts from Information Operations: The Hard Reality of Soft Power, 12.

¹¹ Joint Publication 3-13, vii.

¹² Alan D. Campen, “Information Operations may find definition and validation in Iraq,” Signal 57, no. 10 (June 2003): 43.

¹³ Joint Publication 3-13, viii.

¹⁴ Extracts from Information Operations: The Hard Reality of Soft Power, 13.

¹⁵ Joint Publication 3-13, viii.

¹⁶ E.B. Potter, Extracts from Nimitz Chaper 20 “Return to the Philippines,” Naval War College, Joint Military Operations Department, NWC 2039, 335.

¹⁷ Zachary P. Hubbard, “IO in the Information Age,” Journal of Electronic Defense 27 (April 2004): 51.

¹⁸ Ibid, 54.

¹⁹ Ibid, 55.

²⁰ Ibid, 52.

²¹ Ibid, 52.

²² Joint Publication 3-13, I-4.

²³ U.S. Strategic Command SNAP SHOT, Mission and Capabilities at Snap Shot page.
<<http://www.stratcom.mil/factsheetshtml/SnapShot.doc>> [9 January 2005].

²⁴ “U.S. Strategic Command,” JIOC fact file at Joint Information Operations Center page.
<<http://www.stratcom.mil/FactSheetshtml/Joint%20Info%20Operations%20Center.htm>> [9 January 2005].

²⁵ “U.S. Strategic Command,” JTF-GNO fact file at Joint Task Force – Global Network Operations page.
<<http://www.stratcom.mil/FactSheetshtml/JTF-GNO.htm>> [9 January 2005].

²⁶ Ibid.

²⁷ “U.S. Joint Forces Command,” Mission statement, <<http://www.jfcom.mil>> [9 January 2005].

²⁸ Ibid.

²⁹ Ibid.

³⁰ Ibid.

³¹ Jon Cupp, JFCOM Empowers Warfighters By Setting up Joint Force Headquarters at news link page.
<<http://www.jfcom.mil/newslink/storyarchive/2004/pa031104.htm>> [accessed 8 February 2005].

³² U.S. Joint Forces Command, DRAFT of Standard Operating Procedures & Tactics, Techniques & Procedures for the Standing Joint Force Headquarters (14 July 04) p 44.

³³ JFCOM Empowers Warfighters By Setting Up Joint Force Headquarters. [Accessed 8 February 2005].

³⁴ Ibid.

³⁵ Mark W. Maiers, Timothy L. Rahn, “Information Operations and Millennium Challenge,” Joint Force Quarterly: JFQ (2004) Iss. 35, p 83.

³⁶ Ibid, 84.

³⁷ Ibid, 87.

³⁸ Jpub 3-13, x.

³⁹ Edmund P. Giambastiani, Jr., Admiral, Commander, U. S. Joint Forces Command, (Statement before the House Armed Services Committee U. S. House of Representatives, Washington D.C., March 12, 2003)

⁴⁰ Ibid.

⁴¹ Joint Publication 3-13, I-8 & 9.

⁴² “U.S. Joint Forces Command,” Joint Training Directorate and Joint Warfighting at “Who Works for Us” page. <<http://www.jfcom.mil/about/who.htm>> [9 January 2005].

⁴³ “Joint Warfare Analysis Center,” Mission Statement, <<http://www.jwac.mil/mission.asp>> [8 February 2005].

⁴⁴ Elaine M. Grossman, “Strategic Command to Consolidate Power Over Service-Run Info Ops,” Inside the Pentagon, (28 October 2004).